



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/715,721	11/17/2003	Sunil K. Srivastava	50325-0855	4990

29989 7590 07/14/2005

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER

LAFORGIA, CHRISTIAN A

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 07/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/715,721

Applicant(s)

SRIVASTAVA, SUNIL K.

Examiner

Christian La Forgia

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10 May 2004.
2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) 1-28 is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on 17 November 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 5/29/05, 11/09/04.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____



DETAILED ACTION

1. Claims 1-28 have been presented for examination.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1-11 and 26-28 recites the limitation "the shared secret key value" in the last line of the limitation. There is insufficient antecedent basis for this limitation in the claim. It is unclear whether the Applicant is referring to the initial shared secret key or the subsequent share secret key created by the third node.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-5, 7-15, 17-20, and 22-28 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,668,877 to Aziz, hereinafter Aziz.

6. As per claims 1, 26, and 27, Aziz teaches a method for establishing a secure communication session among a first node of a network and one or more other nodes using a group shared secret key, each of the nodes having a private key value associated therewith, the method comprising the computer-implemented steps of:

communicating a first public key value of the first node to a second node (column 2, lines 20-44, column 8, line 30 to column 9, line 67, i.e. "upon receipt of the encrypted datagram by the

Art Unit: 2131

receiving node J, the node J obtains a DH [Diffie-Hellman] certificate for node I (either from a local cache, from a directory service or directly from node I) and obtains the public value $\alpha^i \bmod p$ ");

creating and storing an initial shared secret key for the first node and second node based on a first private key value and a second public key value that is received from the second node (column 2, lines 20-44, column 4, lines 33-53, column 8, line 30 to column 9, line 67, i.e. "Node I then computes the value $\alpha^j \bmod p$, and derives a key K^{ij} from the value $\alpha^j \bmod p$. A transient key K_p is generated at random and is used to encrypt the datagram to be sent by node I." "The key K_p is then encrypted with key K^{ij} ");

creating and storing information at the first node that associates the first node with a first network communication entity by generating a collective public key value that is shared by the first node and a second node and based on the first private key value and a second private key value that is derived by the first node from the second public key value (column 2, lines 20-44, column 4, lines 33-53, column 8, line 30 to column 9, line 67, i.e. using key pairs in multicast situations);

receiving a third public key value from a third node that seeks to join the first network communication entity (column 4, lines 33-53, column 14, line 3 to column 16, line 58, i.e.

acquiring a new member to join group, similar method as disclosed above);

creating and storing a shared secret key value based on the collective public key value and the third public key value (column 2, lines 20-44, column 4, lines 33-53, column 8, line 30 to column 9, line 67);

Art Unit: 2131

joining the first node to a second network communication entity that includes the first network communication entity and the third node and that uses secure communication with messages that are encrypted using the shared secret key value (column 4, lines 33-53, column 14, line 3 to column 16, line 58, i.e. acquiring a new member to join group).

7. Regarding claims 2 and 12, Aziz teaches wherein joining the first node to a second network communication entity includes the step of communicating the first private key value to the second node and to the third node using messages encrypted using the shared secret key value (column 4, lines 33-53, column 8, line 30 to column 9, line 67, column 14, line 3 to column 16, line 58, i.e. acquiring a new member to join group).

8. Regarding claims 3 and 13, Aziz teaches wherein creating and storing a shared secret key value further comprises creating and storing the shared secret key based upon how many times each node of the second network communication entity has participated in formation of any such entity and based upon each private number of each node in the second network communication entity (column 3, lines 9-50).

9. Regarding claims 4 and 14, Aziz teaches further comprising the step of creating and storing a subsequent shared secret key for use by the first network communication entity and the third node to enable the third node to independently compute the group shared secret key (column 4, lines 33-53, column 8, line 30 to column 9, line 67, column 14, line 3 to column 16, line 58).

10. With regards to claims 5, 15, and 28, Aziz teaches wherein creating and storing the subsequent shared secret key comprises creating and storing the subsequent shared secret key, k , according to the relation

$$k = p^{(a*x)(b*y)(c*z)} \bmod (q)$$

where p = a random number, q = a prime number, a = the first private key value, b = the second private key value, c = a private key value of the third node, x = a number of times the first node has participated in entity formation, y = a number of times the second node has participated in entity formation, and z = a number of times the third node has participated in entity formation (column 3, lines 10-50, column 10, lines 3-40).

11. Concerning claim 7, Aziz teaches wherein the step of joining the first node to a second network communication entity further comprises:

creating and storing a collective public key based upon the first private key value, the second private key value, and the third private key value (column 4, lines 33-53, column 8, line 30 to column 9, line 67, column 14, line 3 to column 16, line 58);

communicating a collective public key of the second network communication entity to the third node (column 4, lines 33-53, column 8, line 30 to column 9, line 67, column 14, line 3 to column 16, line 58).

12. Concerning claims 8 and 22, Aziz discloses wherein the step of joining the first node to a second network communication entity further comprises determining which one of the nodes of the first network communication entity is designated to transfer the collective public key based

Art Unit: 2131

upon order of entry into the formed entity (column 4, lines 33-53, column 14, line 3 to column 16, line 58).

13. Concerning claims 9 and 23, Aziz teaches wherein the step of joining the first node to a second network communication entity further comprises determining which one of the nodes of the first network communication entity is designated to transfer the collective public key based upon a predetermined metric (column 12, line 59 to column 13, line 67).

14. Regarding claims 10 and 19, Aziz teaches wherein creating and storing an initial shared secret key for the first node and second node comprises creating and storing an initial shared public key "AB" according to the relation

$$AB = k_{ab}^{ab} \bmod (q) = p^{(ab)(ab)} \bmod (q)$$

wherein k = the initial shared secret key value, a = the first private key value, b = the second private key value, p is a base value, and q is a randomly generated prime number value (column 3, lines 10-50, column 10, lines 3-40).

15. Regarding claim 17, Aziz teaches wherein the step of joining the first node to a second network communication entity further comprises creating and storing a subsequent collective public key based upon the collective public key value and the first public key value of the first node (column 4, lines 33-53, column 8, line 30 to column 9, line 67, column 14, line 3 to column 16, line 58).

Art Unit: 2131

16. Regarding claim 18, Aziz teaches wherein the step of joining the first node to a second network communication entity further comprises receiving the collective public key from one of the nodes of the first network communication entity that was the first node to join the first network communication entity (column 4, lines 33-53, column 8, line 30 to column 9, line 67, column 14, line 3 to column 16, line 58).

17. Regarding claim 24, Aziz teaches wherein the plurality of nodes communicate over a packet switched network that supports, in part, Internet Protocol (column 2, lines 65-67).

18. Regarding claim 25, Aziz teaches wherein the first node, the second node, and the new node are authenticated by a distributed directory (column 4, lines 33-57).

Claim Rejections - 35 USC § 103

19. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

20. Claims 6, 16, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz in view of U.S. Patent No. 6,295,361 to Kadansky et al., hereinafter Kadansky.

21. Concerning claims 6, 16, and 21, Aziz does not disclose the step of storing and distributing the first public value and the second public value using a key distribution center.

Art Unit: 2131

22. Kadansky teaches the step of storing and distributing the first public value and the second public value using a key distribution center (column 2, lines 1-48). Aziz and Kadansky are related in they both teach the simple key management in Internet protocols.

23. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use a key distribution center, since Kadansky holds at column 2, lines 2-13 that such a modification would alert the multicast group of a change in the group key. One would be motivated to change the group key based on users joining and leaving the multicast group. Aziz supports this motivation in column 1, line 50 to column 2, line 11, in exemplifying the simplicity that a malicious user may gain access to multicast group.

Conclusion

24. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

25. The following patents are cited to further show the state of the art with respect to simple key management in Internet protocols, such as:

United States Patent No. 5,633,933 to Aziz, which is cited to show a key management scheme for Internet protocols.

United States Patent No. 5,588,060 to Aziz, which is cited to show a key management scheme for Internet protocols.

United States Patent No. 6,026,167 to Aziz, which is cited to show a key management scheme for Internet protocols.

United States Patent No. 6,091,820 to Aziz, which is cited to show a key management scheme for Internet protocols.

United States Patent No. 6,049,878 to Caronni et al., which is cited to show efficient, secure multicasting with global knowledge.

United States Patent No. 6,330,671 to Aziz, which is cited to show secure distribution of cryptographic keys on multicast networks.

United States Patent No. 6,606,706 to Li, which is cited to show a hierarchical multicast traffic security system.

United States Patent No. 6,629,243 to Kleinman et al., which is cited to show distributing a key in a multicast communications system.

United States Patent No. 6,785,809 to Hardjono, which is cited to show server group key for distributed group key management for multicast security.

United States Patent No. 6,584,566 to Hardjono, which is cited to show server group key for distributed group key management for multicast security.


26. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

27. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2131

28. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131
Clf


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100